PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 :		(11) Numéro de publication internationale:	WO 00/16557
H04N 7/167, G07F 7/10	A1	(43) Date de publication internationale:	23 mars 2000 (23.03.00)

(21) Numéro de la demande internationale: PCT/FR99/02174

(22) Date de dépôt international: 13 septembre 1999 (13.09.99)

(30) Données relatives à la priorité:
98/11327 11 septembre 1998 (11.09.98) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: THOMSON MULTIMEDIA [FR/FR]; 46, quai Alphonse Le Gallo, F–92100 Boulogne Billancourt (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(US seulement)*: GAUCHE, Laurent [FR/FR]; Thomson multimedia, 46, quai Alphonse Le Gallo, F–92648 Boulogne Cedex (FR).

(74) Mandataire: KOHRS, Martin; Thomson multimedia, 46, quai Alphonse Le Gallo, F–92648 Boulogne Cedex (FR).

(81) Etats désignés: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée

Avec rapport de recherche internationale.
Avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues.

(54) Title: CONDITIONAL ACCESS SYSTEM DECODER AND ENTITLEMENT MANAGEMENT METHOD IN SAME

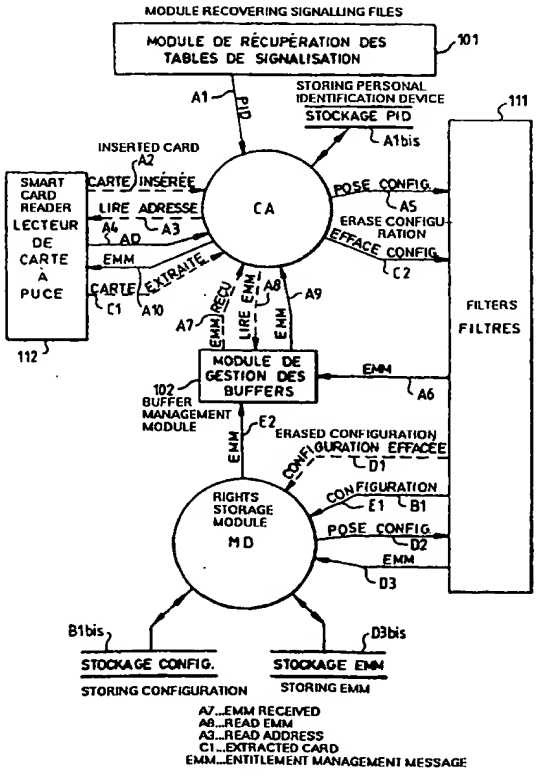
(54) Titre: DECODEUR DE SYSTEME A ACCES CONDITIONNEL ET PROCEDE DE CHARGEMENT DE DROITS D'UTILISATEURS DANS UN TEL DECODEUR

(57) Abstract

The invention concerns a decoder comprising an access control module (CA) capable of recovering on a smart card inserted in the decoder an identification parameter (AD) of the card and setting up a filter configuration for selecting, in the data flow received by the decoder, the entitlement management messages (EMM) addressed to the inserted smart card. The decoder further comprises a rights storage module (MD) capable of storing the configuration set up by the module (CA) and reconstitute said filter configuration when it has been erased, after the smart card has been removed. The messages (EMM) addressed to the smart card can therefore be selected and stored, even when the latter is no longer in the decoder.

(57) Abrégé

Le décodeur comprend un module de contrôle d'accès (CA) capable de récupérer sur une carte à puce insérée dans le décodeur un paramètre d'identification (AD) de la carte et de mettre en place une configuration de filtre permettant de sélectionner, dans le flux de données reçu par le décodeur, les messages de gestion des droits (EMM) destinés à la carte à puce insérée. Il comprend en outre un module de mémorisation des droits (MD) qui est capable de mémoriser la configuration mise en place par le module (CA) et de remettre en place cette configuration de filtre lorsque celle–ci est effacée, suite au retrait de la carte à puce. Les messages (EMM) destinés à la carte à puce peuvent donc être sélectionnés et mémorisés, même lorsqu'elle ne se trouve plus dans le décodeur.



UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	**ES**	Espagne	**LS**	Lesotho	**SI**	Slovénie
AM	Arménie	**FI**	Finlande	**LT**	Lituanie	**SK**	Slovaquie
AT	Autriche	**FR**	France	**LU**	Luxembourg	**SN**	Sénégal
AU	Australie	**GA**	Gabon	**LV**	Lettonie	**SZ**	Swaziland
AZ	Azerbaïdjan	**GB**	Royaume-Uni	**MC**	Monaco	**TD**	Tchad
BA	Bosnie-Herzégovine	**GE**	Géorgie	**MD**	République de Moldova	**TG**	Togo
BB	Barbade	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tadjikistan
BE	Belgique	**GN**	Guinée	**MK**	Ex-République yougoslave de Macédoine	**TM**	Turkménistan
BF	Burkina Faso	**GR**	Grèce			**TR**	Turquie
BG	Bulgarie	**HU**	Hongrie	**ML**	Mali	**TT**	Trinité-et-Tobago
BJ	Bénin	**IE**	Irlande	**MN**	Mongolie	**UA**	Ukraine
BR	Brésil	**IL**	Israël	**MR**	Mauritanie	**UG**	Ouganda
BY	Bélarus	**IS**	Islande	**MW**	Malawi	**US**	Etats-Unis d'Amérique
CA	Canada	**IT**	Italie	**MX**	Mexique	**UZ**	Ouzbékistan
CF	République centrafricaine	**JP**	Japon	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Pays-Bas	**YU**	Yougoslavie
CH	Suisse	**KG**	Kirghizistan	**NO**	Norvège	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	République populaire démocratique de Corée	**NZ**	Nouvelle-Zélande		
CM	Cameroun			**PL**	Pologne		
CN	Chine	**KR**	République de Corée	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Roumanie		
CZ	République tchèque	**LC**	Sainte-Lucie	**RU**	Fédération de Russie		
DE	Allemagne	**LI**	Liechtenstein	**SD**	Soudan		
DK	Danemark	**LK**	Sri Lanka	**SE**	Suède		
EE	Estonie	**LR**	Libéria	**SG**	Singapour		

DECODEUR DE SYSTEME A ACCES CONDITIONNEL ET PROCEDE DE CHARGEMENT DE DROITS D'UTILISATEURS DANS UN TEL DECODEUR.

La présente invention concerne un décodeur de système à accès conditionnel et, plus particulièrement, un procédé de chargement des droits qu'un utilisateur peut acquérir pour accéder à un service distribué au sein d'un système à accès conditionnel.

Un système à accès conditionnel permet à un prestataire de services de ne fournir ses services qu'aux seuls utilisateurs ayant acquis des droits sur ces services. C'est le cas, par exemple, des systèmes de télévision à péage.

Comme cela est connu de l'homme de l'art, le service fourni par un prestataire de services est constitué d'une information embrouillée par des mots de contrôle. Afin de désembrouiller l'information, le prestataire de services fournit à chaque utilisateur les mots de contrôle qui ont servi à embrouiller l'information. De façon à garder secrets les mots de contrôle, ceux-ci sont fournis après avoir été chiffrés avec un algorithme de clé K. Les différents mots de contrôle chiffrés sont envoyés aux différents utilisateurs dans des messages de contrôle communément notés ECM (l'abréviation ECM provient de l'anglais "Entitlement Control Message"). Les mots de contrôle sont déchiffrés dans un processeur sécurisé contenu dans un élément de sécurité tel que, par exemple, une carte à puce.

L'information embrouillée ne peut être désembrouillée, et donc lue par un utilisateur, qu'à hauteur des droits attribués à cet utilisateur. Les droits de chaque utilisateur sont envoyés dans des messages de gestion des droits communément notés EMM (l'abréviation EMM est issue de l'anglais "Entitlement Management Message"). Le processeur sécurisé permet de valider et d'enregistrer les droits qu'a l'utilisateur sur le service délivré.

Selon un exemple de réalisation connu de système à accès conditionnel, le prestataire de services fournit à chaque utilisateur une carte à puce et un décodeur. La sélection des messages EMM s'effectue par la mise en place d'une configuration appropriée de filtres contenus dans le

décodeur. Cette configuration est mise en place à partir de la lecture, par des circuits du décodeur, de données contenues dans la carte à puce. A cette fin, l'utilisateur est amené à introduire la carte à puce dans le décodeur.

Quand les messages EMM qui correspondent à la carte à puce sont présents dans le signal que reçoit le décodeur, ils sont sélectionnés à l'aide des filtres et transférés vers la carte à puce où les droits correspondants sont mis à jour et mémorisés.

Les messages EMM sont émis, de façon asynchrone, avant l'émission du service embrouillé auquel ils correspondent. Les droits utilisateur sont ainsi, par exemple, très souvent émis aux heures les plus creuses de la nuit. Par ailleurs, les droits utilisateur sont amenés à être fréquemment renouvelés sans que l'utilisateur en ait la connaissance.

Il s'ensuit qu'un utilisateur qui désire pouvoir utiliser régulièrement les services d'un prestataire se trouve pratiquement dans l'obligation de laisser en permanence la carte à puce que lui a fourni le prestataire dans le décodeur pour que le transfert des messages EMM du décodeur vers la carte à puce puisse être effectué dès que possible.

Un utilisateur qui est abonné à plusieurs prestataires de services possède autant de cartes à puce qu'il a d'abonnements. Au cas où les différents prestataires de services partagent le même décodeur, on peut envisager de prévoir plusieurs lecteurs de cartes à puces différents sur le même décodeur mais dans ce cas, cela augmente notablement le prix du décodeur. Dans le cas plus probable où l'utilisateur possède plus de cartes à puces que de lecteurs de cartes disponibles sur son décodeur, il lui est alors quasiment impossible de gérer correctement son parc de cartes à puce pour acquérir dès que possible l'ensemble des droits auxquels il peut prétendre.

L'invention vise à résoudre les problèmes précités.

Elle concerne à cet effet un décodeur de système à accès conditionnel comprenant :

- au moins un dispositif destiné à lire et/ou à écrire des données dans un élément de sécurité détachable fourni par un prestataire de service;

- des filtres destinés à sélectionner au moins un message de gestion des droits qu'un utilisateur possède sur un service fourni par le prestataire parmi un flot de données reçu; et

- un module de contrôle d'accès qui est capable de recevoir un paramètre d'identification contenu dans un élément de sécurité inséré dans le décodeur; de mettre en place une configuration de filtre en fonction du paramètre d'identification reçu de façon à sélectionner un message de gestion des droits destiné à cet élément de sécurité inséré; et de transmettre ledit message audit élément de sécurité inséré.

Selon l'invention, le décodeur comporte en outre un module de mémorisation des droits qui est capable de mémoriser la configuration de filtres mise en place par le module de contrôle d'accès précité; de remettre en place, suite à l'effacement de la configuration de filtres consécutive au retrait de l'élément de sécurité, la configuration de filtres mémorisée appropriée audit élément de sécurité, de façon à sélectionner un message de gestion des droits destiné audit élément de sécurité lorsque ce dernier est retiré; et de mémoriser ledit message dans une mémoire du décodeur.

Selon un autre aspect de l'invention, le module de mémorisation des droits du décodeur est en outre capable de détecter l'insertion d'un élément de sécurité dans le décodeur; de vérifier si un message de gestion des droits destiné audit élément de sécurité inséré est mémorisé dans la mémoire du décodeur; et en cas de vérification positive, de transférer ledit message mémorisé audit élément de sécurité inséré.

Selon un mode de réalisation préféré de l'invention, le module de mémorisation des droits détecte l'insertion d'un élément de sécurité dans le décodeur en enregistrant toute nouvelle mise en place de configuration de filtres par le module de contrôle d'accès.

L'invention concerne également un procédé de traitement de message de gestion des droits qu'un utilisateur possède sur un service, ledit procédé comprenant les étapes consistant à :

- insérer un élément de sécurité détachable dans un décodeur;

- récupérer dans ledit élément de sécurité un paramètre d'identification;

- mettre en place une configuration de filtre du décodeur en fonction dudit paramètre d'identification de façon à sélectionner un message de gestion des droits destiné audit élément de sécurité inséré;

- transmettre ledit message audit élément de sécurité inséré.

Selon l'invention, l'étape de mise en place de la configuration de filtre appropriée audit élément de sécurité est suivie d'une étape de mémorisation de ladite configuration et, lorsque ledit élément de sécurité est retiré du décodeur, provoquant l'effacement de ladite configuration de filtres, la configuration de filtres appropriée à l'élément de sécurité retiré est remise en place à partir de la configuration mémorisée lors de l'étape de mémorisation de façon à sélectionner un message de gestion des droits destiné audit élément de sécurité retiré.

Selon un aspect préféré de l'invention, le procédé comporte une étape supplémentaire consistant à mémoriser dans une mémoire du décodeur le message de gestion des droits destiné à l'élément de sécurité retiré lorsqu'un tel message est sélectionné.

Selon un autre aspect de l'invention, le procédé comporte en outre les étapes consistant à :

- réinsérer l'élément de sécurité dans le décodeur;

- vérifier si un message de gestion des droits destiné audit élément de sécurité inséré est mémorisé dans la mémoire du décodeur; et

- en cas de vérification positive, transférer ledit message mémorisé audit élément de sécurité inséré.

Un avantage de l'invention est de permettre l'acquisition de droits utilisateur sans que l'élément de sécurité qui contient les données pour mettre en place la configuration de filtres permettant l'acquisition de ces droits ne soit présent dans le décodeur au moment de l'acquisition.

D'autres caractéristiques et avantages de l'invention apparaîtront à la lecture d'un mode de réalisation particulier, non limitatif, de l'invention fait en référence aux figures 1 à 4, parmi lesquelles:

- la figure 1 représente un décodeur muni d'un élément de sécurité selon l'invention;

- la figure 2 représente schématiquement un paquet de données transportant un message de gestion des droits d'un utilisateur;

- la figure 3 représente schématiquement les différents évènements et les différents transferts de données intervenant durant le procédé de traitement des messages de gestion des droits utilisateur selon l'invention;

- les figures 4a à 4e illustrent différentes étapes du procédé selon l'invention.

Sur toutes les figures, les mêmes références désignent les mêmes éléments.

La figure 1 représente un décodeur de système à accès conditionnel permettant à un utilisateur chez qui il est installé de recevoir des services, tels que des programmes télévisés, sous forme de flux d'information numérique codé par exemple selon la norme MPEG 2 (ISO/IEC 13818-1).

Seuls les éléments nécessaires à la compréhension de l'invention ont été représentés à la figure 1.

Le décodeur comporte de manière connue en soi un tuner/démodulateur 17 qui reçoit un signal S, issu d'une antenne satellite ou d'un réseau câblé, et qui fournit en sortie un flux de données numériques, transmis sous forme de paquets, appelé TS (de l'anglais "Transport Stream" signifiant "flux de transport") dans la norme MPEG 2 précitée, et contenant les services fournis par des prestataires.

Les services étant transmis sous forme embrouillée, chaque prestataire de service fournit également à l'utilisateur une carte à puce 10 qui contient des éléments secrets permettant de désembrouiller les services.

Cette carte à puce 10 est destiné à être insérée dans un lecteur de carte à puce du décodeur dont on a représenté uniquement l'interface 12 avec un microcontrôleur 16 dans lequel sont exécutés les différentes applications du décodeur.

Le décodeur comporte également une mémoire 14 à laquelle le microcontrôleur 16 peut accéder en lecture ou en écriture.

Enfin, le décodeur comprend un composant 20 appelé démultiplexeur qui reçoit le flux de données TS pour en extraire les paquets de données vidéo ou audio correspondant à un service que l'utilisateur désire visualiser ou pour en extraire des paquets de données contenant des informations dites "de service", telles que des messages EMM de gestion des droits utilisateur.

Le démultiplexeur 20 est composé de filtres 11 et d'une mémoire tampon 18, appelée généralement "buffer".

Les filtres sont formés, comme cela est connu de l'homme de l'art, d'ensembles de comparateurs recevant d'une part le flux de données TS et d'autre part une valeur de référence permettant d'identifier les paquets de données à extraire. Lorsque des paquets de données sont extraits du flux TS, ceux-ci sont stockés dans le buffer 18 avant d'être utilisés par les différentes applications du décodeur qui sont exécutées dans le microcontrôleur 16.

A la figure 2, on a représenté un paquet de données contenant un message EMM de gestion des droits utilisateur. Comme tout paquet de données transporté dans le flux TS, il comporte un identifiant : le PID (de l'anglais "Packet IDentifier"), suivi de données dites "privées". En effet, toutes les données concernant le contrôle d'accès sont spécifiques au prestataire de service et ne sont pas définies dans la norme de transport des paquets de données.

Dans les données privées se trouve le message EMM proprement dit. Ce message se compose de trois éléments :

- un premier élément AD contenant l'adresse de la carte à puce à laquelle est destiné le message EMM; il peut également s'agir d'une adresse correspondant à un groupe de cartes à puces auxquelles est destiné le message EMM;
- un second élément contenant les droits de l'utilisateur (abonnement, jetons pour un achat impulsif de programme, etc...); et
- un troisième élément SIGN permettant de valider le contenu du message EMM qui ne sera pas décrit plus avant.

Lorsqu'un message EMM destiné à la carte à puce 10 qui est insérée dans le décodeur doit être extrait du flux de données TS, il est donc nécessaire de configurer un filtre en lui fournissant comme valeur de référence le PID des paquets de données transportant les messages EMM et l'adresse de la carte à puce qui se trouve dans le décodeur.

Dans la suite, on dira que l'on "met en place" ou que l'on "pose" une configuration de filtre pour signifier que l'on transmet à un filtre les paramètres précités (PID, adresse carte à puce) permettant de sélectionner un message EMM destiné à une carte à puce donnée.

Nous allons maintenant décrire plus en détail, en liaison avec les figures 3 et 4, le mécanisme de récupération des messages EMM destinés à une carte à puce donnée dans le flux TS reçu.

Sur la figure 3, nous avons représenté sous forme de rectangles les différentes ressources, partagées par toutes les applications du décodeur, qui sont utiles à la compréhension de l'invention. Ces ressources partagées comprennent:

- des filtres 111, qui correspondent aux filtres 11 de la figure 1;
- un module lecteur de carte à puce 112 qui comprend à la fois une partie matérielle (le circuit de lecture/écriture sur la puce - ou circuit intégré - de la carte) et une partie logicielle permettant de communiquer avec les autre applications du décodeur;
- un module dit de récupération des tables de signalisation 101 qui est un logiciel capable d'extraire du flux TS des tables contenant des informations sur la structure et le positionnement des paquets de données dans le flux TS. Notamment, ce module est capable d'extraire une table appelée CAT (de l'anglais "Conditional Access Table" signifiant littéralement "table d'accès conditionnel") dans la norme MPEG 2 précitée et qui contient, entre autres, les PID identifiant les paquets de données contenant les messages EMM;
- un module de gestion des buffers qui est un logiciel bas niveaux chargé d'allouer et de manipuler les buffers utilisés pour le stockage des paquets qui sont extraits du flux de données TS par les filtres 111.

Les différentes ressources qui viennent d'être décrites sont utilisées par des applications (des logiciels) qui sont représentées par des cercles à la figure 3. Enfin, sur la figure 3, on a représenté les flux de données par des flèches continues et les évènements par des flèches en pointillés.

Nous nous intéresserons dans la suite uniquement aux applications qui sont utiles au chargement des droits utilisateur dans le cadre de l'invention.

La première application, le module CA est un logiciel spécifique à un prestataire de service et qui implémente le système d'accès conditionnel de ce prestataire. En effet, il est très rare que deux prestataires de services différents utilisent le même système d'accès conditionnel. En général, le module CA est donc un logiciel secret, qui n'est connu que du prestataire de service. Le fabriquant de décodeur le reçoit sous forme de "code objet" (logiciel compilé non compréhensible – par opposition au "code source" – et non modifiable tel quel) pour être intégré au décodeur.

La deuxième application, appelée module de mémorisation des droits MD, est, selon l'invention, un module applicatif indépendant du module CA avec lequel il ne communique pas directement. Le rôle de ce module MD est, comme on le verra ci-dessous, "d'espionner" les configurations de filtres mises en place par le module CA pour être ensuite capable de recevoir des messages EMM destinés à une carte à puce qui a été extraite du décodeur à la place du module CA.

Nous allons maintenant décrire plus précisément les différentes étapes conduisant au chargement des droits de l'utilisateur sur sa carte à puce.

Lorsque l'utilisateur du décodeur sélectionne un service particulier, par exemple une chaîne télévisée, le module de récupération des tables de signalisation 101 récupère la table CAT décrite ci-dessus et le module CA récupère dans cette table (étape A1, Fig. 3) le PID identifiant les paquets de données dans lesquels sont transmis les messages EMM pour le prestataire fournissant le service sélectionné. Le PID est ensuite stocké par

le module CA dans la mémoire 14 du décodeur (étape "STOCKAGE PID" A1bis).

Si nous supposons qu'une carte à puce No. 1 est insérée dans le décodeur, alors le module lecteur de carte 112 génère un événement "CARTE INSEREE" à l'étape A2. A la réception de cet événement, le module CA génère un événement "LIRE ADRESSE" à l'étape A3 et obtient, en réponse du module lecteur de carte 112, l'adresse de la carte à puce à l'étape A4.

A l'aide de cette adresse et du PID stocké, le module CA peut mettre en place une configuration de filtres C1 pour sélectionner les messages EMM destinés à la carte à puce No. 1 (étape A5 "POSE CONFIG.").

En se reportant maintenant à la figure 4a, on a représenté l'ensemble 111 des filtres F1 à Fn disponibles pour les différentes applications du décodeur. On suppose que le filtre F1 est alloué à une autre application, il est donc représenté de manière hachurée à la figure 4a. Le premier filtre disponible est le filtre F2. Celui-ci est alloué au module CA qui met donc en place la configuration C1 dans F2.

En revenant à la figure 3, on suppose maintenant qu'un paquet contenant un message EMM a été sélectionné par le filtre F2 qui le transmet (étape A6) au module pilote 102, lequel génère un événement "EMM RECU" à l'attention du module CA (étape A7) qui répond par un événement "LIRE EMM" (étape A8) avant de recevoir le message EMM correspondant (étape A9). Le module CA transmet enfin le message EMM au module lecteur de carte 112 (étape A10) pour que ce dernier le transfère à la carte à puce No. 1 pour traitement (mise à jour des droits de l'utilisateur mémorisés dans la carte). Les étapes A6 à A10 sont répétées autant de fois que des messages EMM destinés à la carte à puce No. 1 sont reçus par le filtre F2.

En considérant maintenant le module MD de l'invention, celui-ci surveille en permanence les configurations de filtres qui sont mises en place par le module CA et, dès qu'une nouvelle configuration est posée, comme à l'étape A5 précitée, le module MD récupère cette configuration (étape B1) pour la mémoriser (étape "STOCKAGE CONFIG." B1bis). A la figure 4a, on

se trouve à la fin de cette dernière étape et on constate que la configuration C1 mise en place par le module CA a été mémorisée par le module MD (voir tableau "STOCKAGE MD", colonne "CONFIG.").

Supposons maintenant que l'utilisateur retire la carte à puce No. 1. Un événement "CARTE EXTRAITE" est alors généré par le module lecteur de carte 112 (étape C1). A la réception de cet événement, le module CA efface la configuration de filtre C1 correspondant à la carte retirée (étape C2). Le filtre F2 est donc libéré (Figure 4b).

Le module MD qui surveille les filtres 111 reçoit alors un événement "CONFIGURATION EFFACEE" (étape D1) et remet aussitôt en place (étape D2) ladite configuration C1 qui avait été mémorisée à l'étape B1bis précédente. A la figure 4b, on a ainsi représenté l'état des filtres à l'issue de cette étape D2: le filtre F1 est toujours alloué à une autre application du décodeur; le filtre F2 a été libéré par le module CA et le filtre Fi a été alloué au module MD pour mettre en place la configuration C1.

On notera pour la suite que lorsqu'un filtre est alloué au module CA, il est représenté sur les figures 4a à 4e par un rectangle en traits gras continus, alors que lorsqu'un filtre est alloué au module MD, il est représenté par un rectangle en traits gras pointillés.

Grâce au module MD de l'invention, les messages EMM destinés à la carte à puce No. 1 peuvent donc encore être sélectionnés dans le flux de données TS par le filtre Fi malgré l'absence de ladite carte dans le décodeur. Lorsqu'un tel message EMM destiné à la carte No. 1 est sélectionné, il est transmis au module MD (étape D3) pour être mémorisé dans une mémoire du décodeur (étape "STOCKAGE EMM" D3bis). Avantageusement, les messages EMM sont mémorisés dans une zone de mémoire tampon temporaire de la mémoire 14 du décodeur.

En se reportant à la figure 4c, on suppose qu'une carte à puce No. 2 est insérée dans le décodeur. Le filtre F2 est donc alloué au module CA pour mettre en place une configuration C2 permettant de sélectionner des messages EMM destinés à la carte No. 2. Cette configuration C2 est aussitôt mémorisée par le module MD (voir tableau "STOCKAGE MD", colonne "CONFIG."). En parallèle, le filtre Fi reste alloué au module MD avec

la configuration C1 pour récupérer les messages EMM destinés à la carte à puce No. 1 qui a été extraite. On suppose qu'à la fin de cette étape, un message EMM1 destiné à la carte No. 1 a été mémorisé par le module MD (voir colonne "EMM" du tableau "STOCKAGE MD").

A la figure 4d, on suppose que la carte No. 2 a été extraite, le filtre F2 est donc à nouveau libéré et le filtre F1 qui se trouvait libre a été alloué au module MD pour mettre en place la configuration C2 mémorisée précédemment. Le filtre Fi reste quant à lui toujours alloué au module MD avec la configuration C1.

Supposons maintenant que l'utilisateur réinsère sa carte à puce No. 1 dans le décodeur. Les étapes A2 à A5 décrites précédemment sont alors exécutées et un filtre, par exemple le filtre F2 (Figure 4e), est alloué au module CA avec la configuration C1. Le module MD, qui surveille en permanence les configurations de filtres mises en place par le module CA, reçoit cette configuration C1 (étape E1) et la compare avec celles déjà mémorisées (C1, C2). Comme cette configuration C1 est déjà mémorisée, le module MD vérifie ensuite si des messages EMM destinés à la carte à puce No. 1 correspondante sont mémorisés et il trouve le message EMM1.

Le message EMM1 est alors transmis au module pilote 102 (étape E2) comme s'il parvenait directement des filtres 111 (comme lors de l'étape A6). Les étapes A7 à A10 sont alors rejouées et tout se passe, du point de vue du module CA, comme si le message EMM1 reçu venait d'être sélectionné par le filtre F2 dans le flux de données TS.

Ainsi, grâce à l'invention, la mise à jour des droits de l'utilisateur pour la carte No. 1 est faite même si les nouveaux droits ont été reçus alors que la carte ne se trouvait pas insérée dans le décodeur. En outre, un avantage important du module MD de l'invention est qu'il intervient sur les différentes ressources du décodeur sans jamais interagir directement avec le module CA. Le logiciel du module CA n'a donc pas à être modifié par rapport aux décodeurs de l'art antérieur.

Lorsque le message EMM1 est transmis au module pilote 102 par le module MD, ce dernier libère en même temps l'espace mémoire réservé pour mémoriser le message EMM1 (voir colonne "EMM" du tableau

"STOCKAGE MD", Fig. 4e). A la figure 4e, on retrouve en outre le filtre F1 qui est alloué au module MD avec la configuration C2 et on suppose qu'un message EMM2 destiné à la carte à puce No. 2 a été reçu et mémorisé (voir colonne "EMM" du tableau précité).

En ce qui concerne la stratégie de libération des filtres, celle-ci dépend de l'implémentation choisie par le développeur du décodeur. Par exemple, on peut choisir comme à la figure 4e de libérer le filtre Fi (qui était auparavant alloué au module MD avec la configuration C1) dès qu'un autre filtre (ici F2) est alloué avec la même configuration que Fi.

La description du mode de réalisation préféré de l'invention a été faite en utilisant l'exemple de la norme de transport de paquets de données numérique MPEG 2 mais l'invention s'applique naturellement dans le cadre de toute autre norme de transport de données.

REVENDICATIONS

1. Décodeur (9) de système à accès conditionnel comprenant :

- au moins un dispositif (12) destiné à lire et/ou à écrire des données dans un élément de sécurité détachable (10) fourni par un prestataire de service;

- des filtres (11) destinés à sélectionner au moins un message (EMM) de gestion des droits qu'un utilisateur possède sur un service fourni par ledit prestataire parmi un flot de données (TS) reçu;

- un module de contrôle d'accès (CA) capable de :

a) recevoir un paramètre d'identification (AD) contenu dans un élément de sécurité (10) inséré dans ledit décodeur;

b) mettre en place une configuration (C1, C2) de filtre en fonction du paramètre d'identification (AD) reçu de façon à sélectionner un message de gestion des droits (EMM) destiné audit élément de sécurité (10) inséré; et

c) transmettre ledit message (EMM) audit élément de sécurité inséré;

caractérisé en ce qu'il comporte en outre :

- un module de mémorisation des droits (MD) capable de :

i) mémoriser ladite configuration de filtres (C1, C2) mise en place par le module de contrôle d'accès (CA);

ii) remettre en place, suite à l'effacement de la configuration de filtres consécutive au retrait dudit élément de sécurité, la configuration de filtres mémorisée appropriée audit élément de sécurité, de façon à sélectionner un message de gestion des droits (EMM) destiné audit élément de sécurité lorsque ce dernier est retiré; et

iii) mémoriser ledit message (EMM) dans une mémoire (14) dudit décodeur.

2. Décodeur selon la revendication 1, dans lequel le module de mémorisation des droits (MD) est en outre capable de :

iv) détecter l'insertion d'un élément de sécurité dans ledit décodeur;

v) vérifier si un message de gestion des droits (EMM) destiné audit élément de sécurité inséré est mémorisé dans la mémoire (14) du décodeur; et

vi) en cas de vérification positive, transmettre ledit message (EMM) mémorisé audit élément de sécurité inséré.

3. Décodeur selon la revendication 2, dans lequel le module de mémorisation des droits (MD) détecte l'insertion d'un élément de sécurité (10) dans le décodeur en enregistrant toute nouvelle mise en place de configuration de filtres par le module de contrôle d'accès (CA).

4. Décodeur selon l'une des revendications 1 à 3, dans lequel l'élément de sécurité détachable (10) est une carte à puce.

5. Décodeur selon la revendication 4, dans lequel le paramètre d'identification (AD) contenu dans l'élément de sécurité est l'adresse de la carte à puce.

6. Procédé de traitement de message (EMM) de gestion des droits qu'un utilisateur possède sur un service, ledit procédé comprenant les étapes consistant à :

- insérer un élément de sécurité détachable (10) dans un décodeur (9);
- récupérer (A3, A4) dans ledit élément de sécurité un paramètre d'identification (AD);
- mettre en place (A5) une configuration de filtre du décodeur en fonction dudit paramètre d'identification (AD) de façon à sélectionner un message de gestion des droits (EMM) destiné audit élément de sécurité inséré;
- transmettre (A6-A10) ledit message (EMM) audit élément de sécurité inséré,

caractérisé en ce que l'étape de mise en place de la configuration de filtre appropriée audit élément de sécurité est suivie d'une étape de mémorisation (B1, B1bis) de ladite configuration et en ce que, lorsque ledit élément de sécurité (10) est retiré du décodeur, provoquant l'effacement (C2) de ladite configuration de filtres, la configuration de filtres appropriée à l'élément de sécurité retiré est remise en place (D2) à partir de la configuration mémorisée lors de l'étape de mémorisation de façon à sélectionner un message de gestion des droits (EMM) destiné audit élément de sécurité retiré.

7. Procédé selon la revendication 4, caractérisé en ce qu'il comporte une étape supplémentaire (D3, D3bis) consistant à mémoriser dans une mémoire (14) du décodeur ledit message de gestion des droits (EMM) destiné audit élément de sécurité retiré lorsqu'un tel message est sélectionné.

8. Procédé selon la revendication 5, caractérisé en ce qu'il comporte en outre les étapes consistant à :

- réinsérer ledit élément de sécurité (10) dans le décodeur;
- vérifier si un message de gestion des droits (EMM) destiné audit élément de sécurité inséré est mémorisé dans la mémoire (14) du décodeur; et
- en cas de vérification positive, transférer ledit message (EMM) mémorisé audit élément de sécurité inséré.

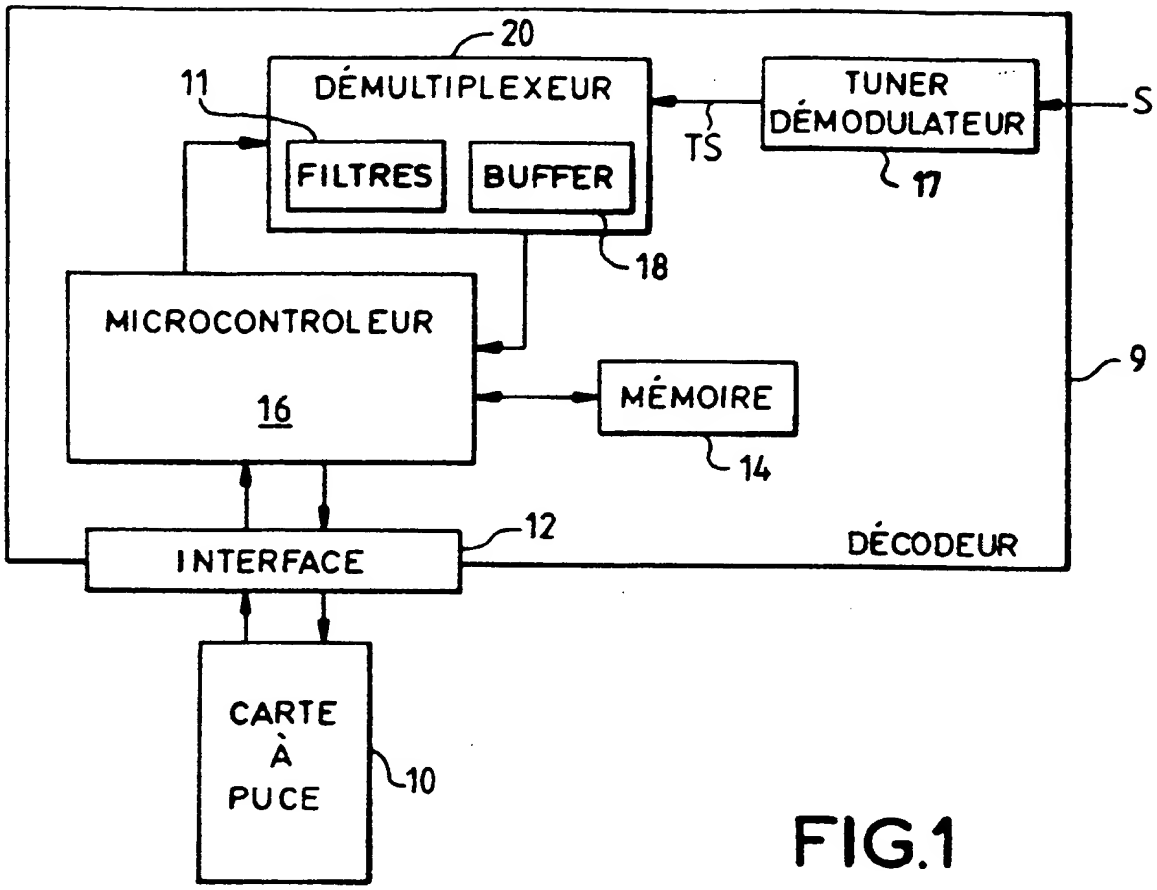

20
11
DÉMULTIPLEXEUR
FILTRES
BUFFER
TS
TUNER
DÉMODULATEUR
S
17
18
MICROCONTROLEUR
16
MÉMOIRE
14
9
12
INTERFACE
DÉCODEUR
CARTE
À
PUCE
10

FIG.1

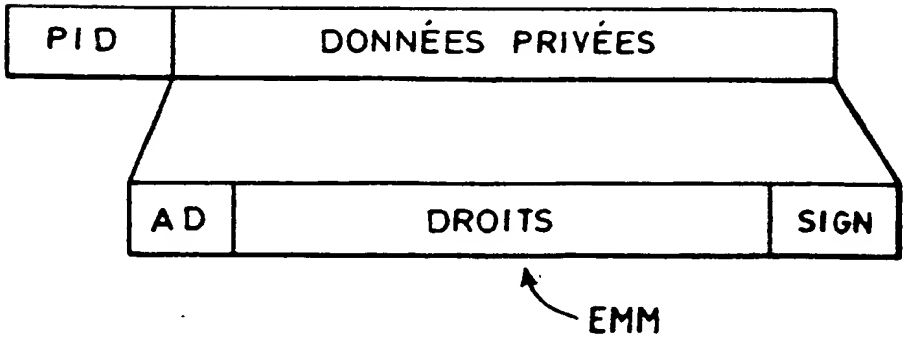

PID
DONNÉES PRIVÉES
AD
DROITS
SIGN
EMM

FIG.2

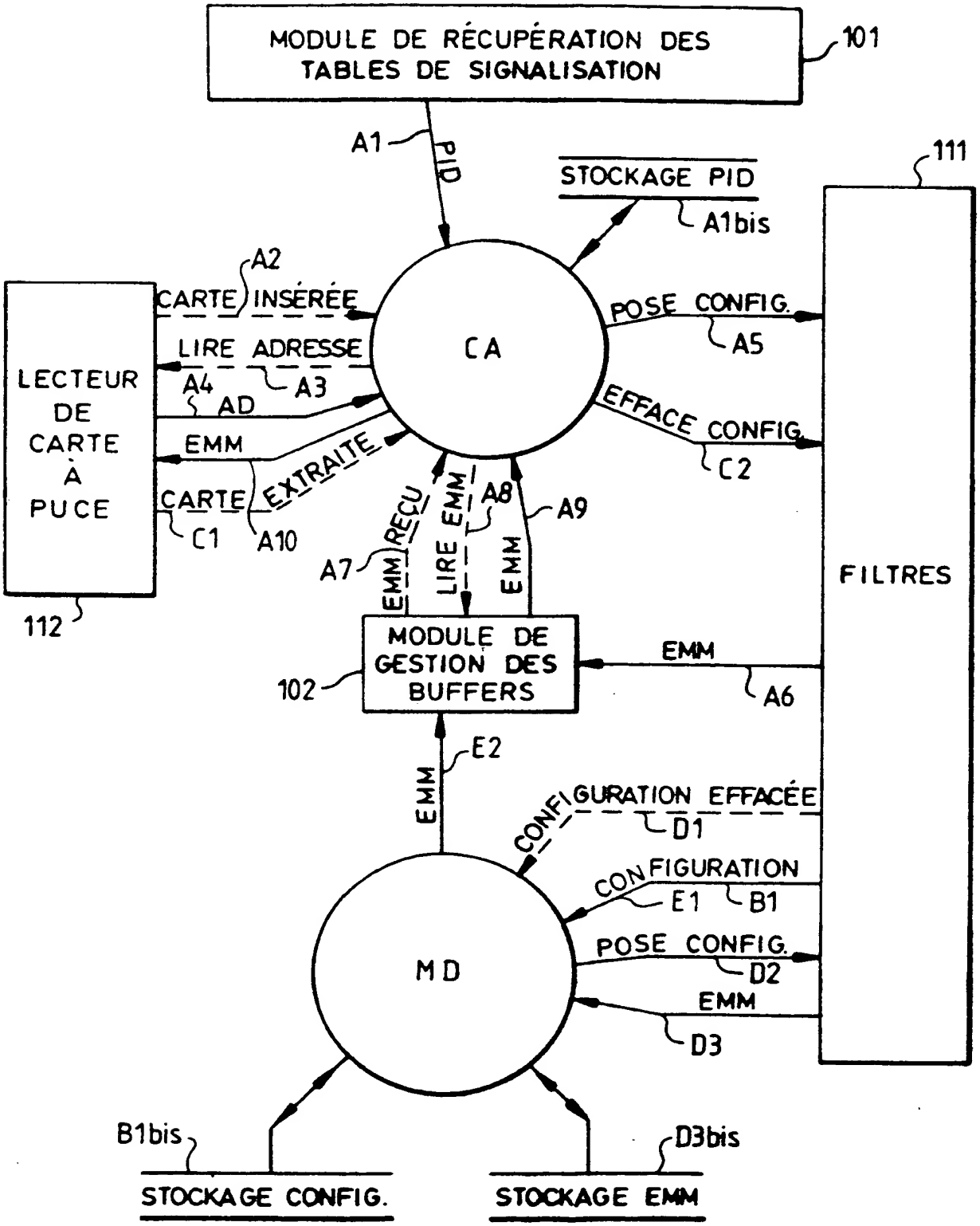

MODULE DE RÉCUPÉRATION DES TABLES DE SIGNALISATION
101
A1
PID
STOCKAGE PID
A1bis
111
A2
CARTE INSÉRÉE
LECTEUR DE CARTE À PUCE
LIRE ADRESSE
A4
AD
A3
EMM
CARTE
C1
EXTRAITE
A10
CA
POSE CONFIG.
A5
EFFACE CONFIG.
C2
A7
EMM
REÇU
LIRE EMM
A8
EMM
A9
FILTRES
112
MODULE DE GESTION DES BUFFERS
102
EMM
A6
E2
EMM
CONFIGURATION EFFACÉE
D1
CONFIGURATION
E1
B1
POSE CONFIG.
D2
EMM
D3
MD
B1bis
STOCKAGE CONFIG.
D3bis
STOCKAGE EMM

FIG.3

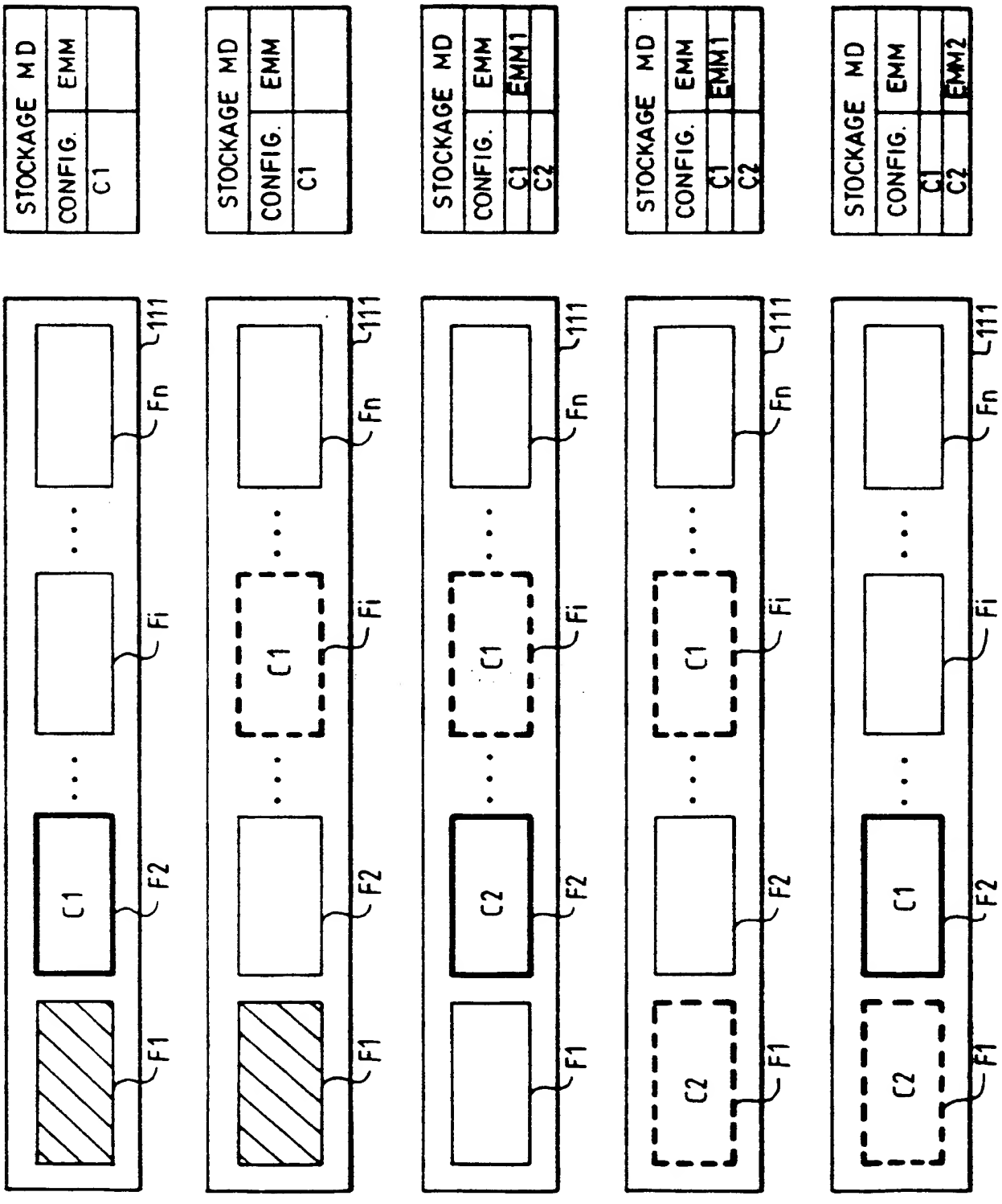


FIG.4a FIG.4b FIG.4c FIG.4d FIG.4e

INTERNATIONAL SEARCH REPORT

[redacted] onal Application No
PCT/FR 99/02174

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/167 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SCHOONEVELD VAN D: "STANDARDIZATION OF CONDITIONAL ACCESS SYSTEMS FOR DIGITAL PAY TELEVISION" PHILIPS JOURNAL OF RESEARCH, vol. 50, no. 1/02, 1 July 1996 (1996-07-01), pages 217-225, XP000627672 page 218, line 12 -page 219, line 10 ---	1,6
A	EP 0 817 485 A (THOMSON MULTIMEDIA SA) 7 January 1998 (1998-01-07) abstract; claims; figures ---	1,6
A	WO 98 09257 A (GEMPLUS CARD INT) 5 March 1998 (1998-03-05) abstract; claims; figures page 7, line 12 -page 8, line 18 ---	16

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 December 1999	12/01/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Meyl, D

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

[redacted]onal Application No
[redacted]/FR 99/02174

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 723 371 A (THOMSON MULTIMEDIA SA) 24 July 1996 (1996-07-24) abstract; figures	1,6
A	WO 96 06504 A (CHANEY JOHN WILLIAM ;THOMSON CONSUMER ELECTRONICS (US)) 29 February 1996 (1996-02-29) abstract; figures	1,6
A	COUTROT F ET AL: "A SINGLE CONDITIONAL ACCESS SYSTEM FOR SATELLITE-CABLE AND TERRESTRIAL TV" IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, vol. 35, no. 3, 1 August 1989 (1989-08-01), pages 464-468, XP000065971	
A	US 5 619 501 A (CHANEY JOHN W ET AL) 8 April 1997 (1997-04-08)	

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

[redacted]ion on patent family members

[redacted]onal Application No
PCT/FR 99/02174

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0817485 A	07-01-1998	FR 2750554 A	02-01-1998
		CN 1171015 A	21-01-1998
		JP 10164052 A	19-06-1998
WO 9809257 A	05-03-1998	US 5923884 A	13-07-1999
		AU 4842897 A	19-03-1998
		CA 2233217 A	05-03-1998
		EP 0858644 A	19-08-1998
EP 0723371 A	24-07-1996	FR 2729521 A	19-07-1996
		JP 8307850 A	22-11-1996
WO 9606504 A	29-02-1996	AU 3238595 A	22-03-1996
		AU 701593 B	04-02-1999
		AU 3239495 A	14-03-1996
		BR 9508621 A	30-09-1997
		BR 9508622 A	19-05-1998
		CA 2196406 A	07-03-1996
		CA 2196407 A	29-02-1996
		CN 1158202 A	27-08-1997
		CN 1158203 A	27-08-1997
		EP 0878088 A	18-11-1998
		EP 0782807 A	09-07-1997
		FI 970677 A	18-02-1997
		JP 10506507 T	23-06-1998
		JP 10505720 T	02-06-1998
		PL 318647 A	07-07-1997
		WO 9607267 A	07-03-1996
US 5619501 A	08-04-1997	CA 2188127 A	02-11-1995
		CN 1151233 A	04-06-1997
		CN 1167405 A	10-12-1997
		DE 69505369 D	19-11-1998
		DE 69505369 T	15-04-1999
		EP 0756801 A	05-02-1997
		EP 0858222 A	12-08-1998
		ES 2123243 T	01-01-1999
		JP 9512675 T	16-12-1997
		WO 9529560 A	02-11-1995
		US 5802063 A	01-09-1998

RAPPORT DE RECHERCHE INTERNATIONALE

[redacted] le Internationale No
PCT/FR 99/02174

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04N7/167 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultee (système de classification suivi des symboles de classement)
CIB 7 G07F H04N

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultee au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	SCHOONEVELD VAN D: "STANDARDIZATION OF CONDITIONAL ACCESS SYSTEMS FOR DIGITAL PAY TELEVISION" PHILIPS JOURNAL OF RESEARCH, vol. 50, no. 1/02, 1 juillet 1996 (1996-07-01), pages 217-225, XP000627672 page 218, ligne 12 -page 219, ligne 10 ---	1,6
A	EP 0 817 485 A (THOMSON MULTIMEDIA SA) 7 janvier 1998 (1998-01-07) abrégé; revendications; figures ---	1,6
A	WO 98 09257 A (GEMPLUS CARD INT) 5 mars 1998 (1998-03-05) abrégé; revendications; figures page 7, ligne 12 -page 8, ligne 18 ---	16

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
20 décembre 1999	12/01/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Meyl, D

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 0 723 371 A (THOMSON MULTIMEDIA SA) 24 juillet 1996 (1996-07-24) abrégé; figures	1,6
A	WO 96 06504 A (CHANEY JOHN WILLIAM ;THOMSON CONSUMER ELECTRONICS (US)) 29 février 1996 (1996-02-29) abrégé; figures	1,6
A	COUTROT F ET AL: "A SINGLE CONDITIONAL ACCESS SYSTEM FOR SATELLITE-CABLE AND TERRESTRIAL TV" IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, vol. 35, no. 3, 1 août 1989 (1989-08-01), pages 464-468, XP000065971	
A	US 5 619 501 A (CHANEY JOHN W ET AL) 8 avril 1997 (1997-04-08)	

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

e internationale No
PCT/FR 99/02174

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0817485 A	07-01-1998	FR 2750554 A	02-01-1998
		CN 1171015 A	21-01-1998
		JP 10164052 A	19-06-1998
WO 9809257 A	05-03-1998	US 5923884 A	13-07-1999
		AU 4842897 A	19-03-1998
		CA 2233217 A	05-03-1998
		EP 0858644 A	19-08-1998
EP 0723371 A	24-07-1996	FR 2729521 A	19-07-1996
		JP 8307850 A	22-11-1996
WO 9606504 A	29-02-1996	AU 3238595 A	22-03-1996
		AU 701593 B	04-02-1999
		AU 3239495 A	14-03-1996
		BR 9508621 A	30-09-1997
		BR 9508622 A	19-05-1998
		CA 2196406 A	07-03-1996
		CA 2196407 A	29-02-1996
		CN 1158202 A	27-08-1997
		CN 1158203 A	27-08-1997
		EP 0878088 A	18-11-1998
		EP 0782807 A	09-07-1997
		FI 970677 A	18-02-1997
		JP 10506507 T	23-06-1998
		JP 10505720 T	02-06-1998
		PL 318647 A	07-07-1997
		WO 9607267 A	07-03-1996
US 5619501 A	08-04-1997	CA 2188127 A	02-11-1995
		CN 1151233 A	04-06-1997
		CN 1167405 A	10-12-1997
		DE 69505369 D	19-11-1998
		DE 69505369 T	15-04-1999
		EP 0756801 A	05-02-1997
		EP 0858222 A	12-08-1998
		ES 2123243 T	01-01-1999
		JP 9512675 T	16-12-1997
		WO 9529560 A	02-11-1995
		US 5802063 A	01-09-1998